PERFORMANCE WORK STATEMENT (PWS)

Information Assurance and Cyber Security Program Office
PMW 130

Assessment & Authorization (A&A)
Services Contract

October 2019

TABLE OF CONTENTS

1.0 INTRODUCTION

The Program Executive Office (PEO), Command, Control, Communications, Computers, and Intelligence (C4I) is procuring Assessment and Authorization (A&A) and Information System Security Engineering Support Services in support of Program Manager, Warfare (PMW) Information Assurance, and Cyber Security (PMW 130). The purpose of the PWS is to acquire Assessment & Authorization for PMW 130.

1.1 BACKGROUND

Program Executive Office (PEO) Command, Control, Communications, Computers, and Intelligence (C4I) is responsible for the acquisition, integration, delivery, and support of interoperable C4I systems. PMW 130, one of the program offices under PEO C4I, is the Navy's preferred provider of Information Assurance (IA) and Cybersecurity (CS). PMW 130's mission is to acquire and sustain CS products and services to ensure strong authentication, data integrity, confidentiality, non-repudiation, and availability of network resources and information. PMW 130's vision and mission support PEO C4I's strategic objectives in being the U.S. Navy's premier organization for the development, acquisition, and sustainment of C4I capability.

The current CS portfolio consists of the following programs listed in the PWS. Additional programs/projects/initiatives may be added as the CS portfolio is further defined.

1.1.1 Crypto and Key Management

Provide modernized cryptography and associated key delivery infrastructure to Navy, Marine Corps, Coast Guard, and Military Sealift Command to ensure confidentiality of mission critical information.

- Navy Cryptography (Various)
- Key Management (KM), (National Security Agency (NSA) - Acquisition Category (ACAT) IAM)
- Public Key Infrastructure (PKI), (Defense Information Systems Agency (DISA) - ACAT IAM)

1.1.2 Network Security

Deliver products and services that enable the exchange, storage, and processing of data by protecting, monitoring, analyzing, detecting, and responding to unauthorized activity within the DoD information systems and networks of the DoD information networks.

Computer Network Defense (CND) includes systems and host-based protection tools, firewalls, anti-virus, Virtual Private Networks (VPN), email/web content filtering, Intrusion Prevention Systems (IPS), and boundary protection capabilities.

- Computer Network Defense (ACAT IVM)
- SHARKCAGE
- Joint Information Environment/Joint Regional Security Stack
- Deployable Mission Support System – Navy

1.1.3 Cyber Analytics

Provide the Navy with the ability to conduct machine-speed, automated analysis of network activity, and to provide cyber operators with the tools necessary to respond efficiently to cyber-attacks. Cross-domain solutions provide the operators the ability to automatically sanitize and downgrade formatted classified information or transfer information between two or more differing security domains.

- Navy Cyber Situational Awareness

- Cross-domain Solution/Radiant Mercury (AAP)
- Vulnerability and Remediation Asset Manager
- Counter Insider Threat Capability
- Readiness Analytics & Visualization Environment

1.2 SCOPE

The Contractor shall support the Information Security System Manager in the execution of Risk Management Framework (RMF), with Federal Information Security Management Act (FISMA) compliance, program/project Configuration Management, and compliance with NAVWAR Technical Authority products and processes. The scope of this task order includes examination of the system architectures, engineering processes, and cybersecurity functionality.

System architecture includes implementation, reviewing cross system interfaces and systems integration for feasibilities and vulnerabilities, assisting with and observing test and evaluation.

Engineering processes includes verification and validation, engineering analysis, technical documentation analysis, reviewing software and hardware designs.

Cybersecurity functionality includes interfaces, and interoperability of systems of systems, services, and capabilities.

The Contractor shall have the requisite knowledge and experience with fleet operations, IT network security, software and hardware security engineering, and cybersecurity regulations, policy, and strategy. The Contractor shall provide cybersecurity engineering expertise required to ensure system security posture is attained and maintained in accordance with DoD and DON IA/Technical Authority directives, Naval Information Forces (NAVIFOR), and Type Commander (TYCOM) operational guidance. The Contractor shall be familiar with current IA tools and end-to-end processes.

The Contractor shall act as the interface between PEO C4I program offices and the Cross Domain Services (CDS) community by initiating and supporting both GENSER (Navy Cross Domain Service Office (CDSO), Defense Security/Cybersecurity Authorization Working Group (DSAWG), and other component CDSO offices) (Naval Intelligence (NAVINTEL) Information Assurance (NIA) and Defense Intelligence Agency (DIA)) processes; developing documentation templates to cover multiple CDS capabilities managed by a “New CDS” contractor; managing installation and assessment schedules in concert with the “New CDS” contractor; tracking Go/No Go criteria for Site-Based Security Assessments (SBSAs); performing and documenting SBSAs with an Independent Validation and Verification (IV&V) team; supporting Fleet events such as Deploying Group System Integration Testing (DGSIT); tracking PEO C4I program office CDS instantiations as well as their compliance with emergent security issues, patching, and annual recertifications.

2.0 APPLICABLE DOCUMENTS/DIRECTIVES

The following documents were used in the development of this PWS and may be invoked for individual delivery or task orders:

Document Type	**No./Version**	**Title**	**Date**
Cyberspace Policy		Cyberspace Policy Review	May 2009
Presidential Policy Directive	PPD-20	U. S. Cyber Operations Policy, Presidential Policy Directive-20	2010

	PPD-21	Critical Infrastructure Protection and Resilience	12 Feb 2013
Executive Order		Improving Critical Infrastructure Cybersecurity	12 Feb 2013
		International Strategy for Cyberspace	May 2011
		Comprehensive National Cybersecurity Initiative	2008
		The National Security Strategy	December 2017
DoDD	5240.01	DoD Intelligence Activities	22 Mar 2019
DoDD	8530.1	Computer Network Defense	08 Jan 2001
DoDD	O-3600.3	Technical Assurance Standard for Computer Network Attack (CNA) Capabilities	13 May 2005
DoDI	O-3600.3	Technical Assurance Standard for Computer Network Attack (CNA) Capabilities	22 Apr 2010
CJCSM	6510.01B	Cyber Incident Handling Program	10 Jul 12
Joint Doctrine	Joint Pub 3-12	Joint Doctrine for Cyberspace Operations	08 Jun 2018
Joint Doctrine	Joint Pub 3-13	Joint Doctrine for Cyberspace Operations	20 Nov 2014
Naval Warfare Publication	3-12	Cyberspace Operations	8 Jun 2018
Naval Warfare Publication	3-13	Navy Information Operations	1 Feb 2014
Naval Warfare Publication	3-63	CNO Vol 1 and 2	
NTTP	3.13.x Series	Navy Information Operations	
SECNAVINST	5239.19 (Series)	Department of the Navy Computer Network Incident Response and Reporting Requirements	18 May 2008
SECNAVINST	5000.2 (Series)	Defense Acquisition System and Joint Capabilities Integration and Development System Implementation	26 Mar 2019
NAVSEA	3900.8A	Human Systems Integration (HSI) Policy in Acquisition and Modernization	20 May 2005
NIST SP	800-53 (Rev.4)	Security and Privacy Controls for Federal Information Systems and Organizations	January 2015
PMW 130		Organizational Set of Standard Processes	
DoD Manual	5220.22-M (Series)	National Industrial Security Program Operating Manual (NISPOM)	1 Aug 2018
National Security Decision Directive	298	National Operations Security Program (NSDD) 298	22 Jan 1988

DoD	5205.02 (Series)	DOD Operations Security (OPSEC) Program	11 May 2018
OPNAVINST	3432.1 (Series)	DON Operations Security	4 Aug 2011
NAVWARINST	3432.1 (Series)	Operations Security Policy	2 Feb 2005
DoDM	5200.01 Vol 1	DoD Information Security Program: Overview, Classification, And Declassification	04 May 2018
DoDM	5200.01 Vol 2	DoD Information Security Program: Marking Of Classified Information	14 May 2019
DoDM	5200.01 Vol 3	DoD Information Security Program: Protection Of Classified Information	19 Mar 2013
DoDM	5200.01 Vol 4	DoD Information Security Program: Controlled Unclassified Information (CUI)	9 May 2018
DoDI	5200.02	DoD Personnel Security Program (PSP),	11 May 2018
DODM	M-5200.02	Procedures for the DoD Personnel Security Program (PSP)	03 Apr 2017
DoDM	M-5220.22 Vol 2	National Industrial Security Program Operating Manual (NISPOM)	01 Aug 2018
DoDI	5220.22	National Industrial Security Program	01 May 2018
DoDI	6205.02	DOD Immunization Program	23 Jul 2019
DoDI	8500.01	Cybersecurity	14 Mar 2014
DoDI	8510.01	Risk Management Framework (RMF) for DoD Information Technology (IT)	28 Jul 2017
DoDM	8570.01-M	Information Assurance Workforce Improvement Program	19 Apr 2017
DODD	8140.01	Cyberspace Workforce Management	31 Jul 2017
SECNAVINST	M-5239.2	Department Of The Navy Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual	27 Jun 2016
SECNAVINST	M-5510.30	DON Regulation – Personnel Security Program	06 Jun 2006
SECNAVINST	4440.34	Implementation of Item Unique Identification Within the DON	22 Dec 2009
SECNAVINST	5239.3C	DON Cybersecurity Policy	2 May 2016
SECNAVINST	5510.30	DON Regulation – Personnel Security Program	06 Oct 2006
SECNAVINST	5510.36 (Series)	DON Information Security Program	12 Jul 2019
DON CIO Memo		Acceptable Use of Department of	12 Feb 2016

		the Navy Information Technology (IT)	
NAVWARINST	4440.12	Management of Operating Materials and Supplies (OM&S), Government Furnished Property (GFP), Contractor Acquired Property (CAP), Property, Plant and Equipment (PP&E), and Inventory	11 Apr 2016
NAVWARINST	5721.1B	NAVWAR Section 508 Implementation Policy	17 Nov 2009
COMUSFLTFORCOM/ COMPACFLTINST	6320.3A	Medical Screening For US Govt Civilian Employees, Contractor Personnel, and Guests prior to embarking Fleet Units	7 Apr 2014
Navy Telecommunications Directive	NTD 10-11	System Authorization Access Request (SAAR) – Navy	
DoD		DoD Cybersecurity Test and Evaluation Guidebook (Ver 2.0)	February 2018

3.0 PERFORMANCE REQUIREMENTS

The Contactor shall solve complex technical problems. The Contractor shall provide experienced personnel to manage and execute tasks identified in this PWS and perform tasks independently with coordination with Government. The Contractor shall provide monthly Contractor's Progress, Status and Management Reports for each discipline covered by this PWS and in accordance with (IAW) Contract Deliverable Requirements List (CDRL) A001. The Contractor shall work collaboratively with Government personnel and other Contractors internal and external to PMW 130.

The Contractor shall prepare reports and briefings that integrate policy, plans, including requirements, systems engineering, testing, information assurance, and security technology gaps.

Contractor personnel shall be proficient in the use of Microsoft Office Suite (Excel, Word, Access, PowerPoint, Visio, and Project) applications, SPAWAR PEO Integrated Data Environment and Repository (SPIDER), SharePoint, Tableau and Database Management System (DADMS), DoD IT Portfolio Repository (DITPR)-DON, Configuration Management Professional (CMPro), and Enterprise Mission Assurance Support Service (eMASS).

The Contractor shall facilitate or participate in program/project meetings. Meetings include Program Management Reviews (PMRs), Installation Readiness Reviews (IRRs), Test Readiness Reviews (TRRs), Technical Interchange Meetings (TIMs), Integrated Product Team (IPT) meetings, Local Change Control Board (LCCB) meetings, risk assessments, NAVWAR Collaboration meetings, and A&A meetings/discussions related to Cybersecurity programs/projects. The Contractor shall create supporting documentation necessary for participation in meetings.

The Contractor shall draft program briefings, executive summaries, white papers/issue papers, reports, email, and Naval messages. Documentation shall be tailored to the intended audience, based on rank/level, (e.g. Flag/Senior Executive Service (SES) level, Senior Manager/O6, working level, etc.) technical knowledge, location of recipients (e.g. operational Fleet, acquisition command, etc.), and IAW standard guidance.

The Contractor shall be prepared to answer routine A&A questions during meetings, and shall be able to gather data and perform analysis required to close action items. When approved by the Government, the Contractor shall travel to attend meetings.

The Contractor shall prepare and deliver meeting agendas, which outlines the purpose, location, attendees, and schedule and the associated presentation material in the form of slides and or handouts. In addition, the Contractor shall document attendees, significant understandings, recommendations, or suggestions, decisions reached, and action items resulting from discussions in the form of conference/meeting minutes or reports. The Contractor shall submit agendas and presentation materials five days prior to meetings and submit meeting minutes or reports within five days after meetings. (CDRL A001)

3.1 INFORMATION SYSTEM SECURITY MANAGER (ISSM) SERVICES

The Contractor shall:

- Perform required and approved ISSM RMF process steps.
- Document CYBERSAFE requirements, as articulated in OPNAVINST 5239.4.
- Document Cybersecurity T&E requirements in the Test and Evaluation Master Plan (TEMP) as articulated in DoDI 5000.02, Enclosure 14.
- Coordinate RMF and Cybersecurity Test and Evaluation efforts to ensure consistent Cybersecurity findings representation across programs.
- Maintain and report systems' A&A status and issues.
- Develop, track, resolve, and maintain the Security Posture for assigned systems.
- Develop a generation of the programs' CARD and PLCCE to ensure Cybersecurity costs are reflected in a program budget.
- Verify that the generation of a Criticality Analysis to identify mission-critical functions and components that are then documented in the Program Protection Plan.
- Perform the security control implementation and testing.
- Perform security testing required as part of A&A or annual reviews.
- Take actions necessary to mitigate and close open vulnerabilities under the system's change control process.
- Identify and report Cybersecurity gaps to ensure programs are resourced and managed.
- Apply and execute Cybersecurity processes across all levels and phases of an acquisition program/project to deliver products that meets the program/projects requirements and are integrated and interoperable with the Naval Enterprise.
- Identify program Cybersecurity risks and/or issues and recommend mitigation/resolution strategies.

3.2 TECHNOLOGY ASSESSMENT, SYSTEM DEVELOPMENT, AND CYBERSECURITY COMPLIANCE

The Contractor shall work with the system engineers and development team throughout system development activities to determine if developed solutions adhere to RMF Cybersecurity compliance requirements. The Contractor shall evaluate Commercial Off-The-Shelf (COTS), Government Off-The-Shelf (GOTS), and open source technologies, for applicability to Cybersecurity compliance. The contractor shall analyze the technologies proposed as engineering solutions and determine whether their use will enable the system provide assessment of the ability to obtain authorization if the technology is incorporated.

To address the timely challenges of RMF Schedules, the Contractor shall develop system activities and establish RMF authorization schedules. The Contractor shall coordinate RMF Schedules with the PMW 130 Integrated Master Schedules (IMS). In addition, the Contractor shall monitor RMF schedules and provide update in changes to the schedules to the IMS.

3.3 REQUIREMENTS ANALYSIS

The Contractor shall work with the development team to analyze requirements for existing and proposed capabilities to assist with the development of engineered solutions that meet RMF requirements. Identify and derive Cybersecurity requirements at the system and associated architectures to meet RMF compliance. The Contractor shall recommend methods to achieve secure systems while balancing the system capabilities requirements. The Contractor shall assess proposed solution architectures and designs, and strategic roadmaps, and provide recommendations for improvement.

The Contractor shall analyze existing and emerging operational and functional requirements (in the context of Cybersecurity) of existing systems and systems under development, as required by RMF. The Contractor shall work with the system engineers to provide assessment of systems development strategies. The Contractor shall assist engineering and development teams with technical system designs, schedules, and security management plans leading to full system authorizations under RMF. The Contractor shall assist engineering teams with STIG analysis and document negative effects of STIGs on capabilities to balance performance of security controls with operational utility. The Contractor shall analyze STIG requirements and provide feedback to engineering and development team on deficiencies. This includes analysis of software, firmware, hardware (analog and digital sections), as well as protective measures including tamper prevention and implementation methods to detect noncompliance and other malicious threats. The contractor shall assists with the development of corrective actions that meet compliance with RMF standard and ensures systems maintain authorization to operate.

3.4 OPERATIONAL AND TECHNICAL SUPPORT

The Contractor shall review and provide recommended changes to system operational policies including contingency planning, access control, continuity of services, and physical security. Where deficiencies exist, the Contractor shall provide recommendations in writing to the ISSM. The Contractor shall support the development of system policies, and attach appropriate policies for control compliance in eMass.

The Contractor shall conduct technical vulnerability assessments. The Contractor shall develop concepts of operations, standard operating procedures, and technical recommendations that aid the implementation of Memoranda of Understanding or Memoranda of Agreement (MOU/MOA) among accredited system stakeholders. The Contractor shall collaborate with Blue, Green, White, and Red Teams to ensure Cybersecurity compliance and provide recommendations for test events and DoD inspection activities.

The Contractor shall provide training on tools, processes, and procedures. This training shall include STIG applications, STIG tools, RMF, CYBERSAFE, mitigation techniques (identifying solutions and tradeoffs to correct deficiencies), and vulnerability categorization.

The Contractor shall review cybersecurity vulnerability alerts, bulletins, and technical advisories for Transport components per Government (e.g., DoD, DON, National Security Agency (NSA), Defense Information Systems Agency (DISA)) directives, assess against systems and take corrective action and inform the Government if action is required to comply with the recommended guidance.

CDRLs

- A004 Inheritance Memorandum of Agreement (iMOA)

3.5 SECURITY ENGINEERING and CYBERSECURITY

The Contractor shall provide support to the system design engineering and development teams at the earliest possible stages of system development to ensure that IAVA, STIG, vulnerability management, and other protective Cybersecurity concepts have been applied or additional action is necessary to achieve compliance.

The Contractor shall provide security architecture analysis for PMW 130 systems. This includes systems developed by PMW 130 to ensure DoD Cybersecurity compliance, in conjunction with other Navy networks and architectures (including Navy-Marine Corps Intranet (NMCI), Next Generation Enterprise Network (NGEN), Outside the Continental United States (OCONUS) Naval Enterprise Network (ONE-NET), Joint Information Environment (JIE), and Information Dominance Enterprise Architecture (IDEA)).

The Contractor shall verify STIG compliance of major system infrastructure components including firewalls, virtual private network devices, intrusion detection and prevention systems, biometrics technologies, wireless technologies, network vulnerability scanning and remediation technologies, cross domain solutions, and DoD PKI identity and access management systems. The Contractor shall provide security-engineering services to secure private and public Cloud architectures and Cloud applications as a service. The Contractor shall assist the engineering/development teams with implementation of vulnerability detection and correction technologies.

The Contractor shall provide authorization and accreditation expertise in the execution of all Steps of the RMF process. The Contractor shall have knowledge and experience in all phases of the RMF transformation and shall conduct all activities to transition a system from DIACAP to RMF. The Contractor shall plan and execute RMF steps 3 and 4 for PMW 130 systems, providing a schedule and coordination of activities (documented in the schedule), deficiency reporting, and get-well plans. The Contractor shall provide a comprehensive risk assessment to in accordance with RMF steps 3 through 6. The Contractor shall facilitate and track all documentation associated with A&A requirements. The Contractor shall prepare system policy documentation for developmental and fielded systems. The Contractor shall identify systems under DIACAP, provide risk assessments, and develop RMF transition plans. The Contractor shall analyze security test plans, procedures, and reports. The Contractor shall provide dedicated ISSE support to the In-Service Engineering Agent (ISEA) and to the development activity. The Contractor shall serve as a liaison between the system development teams and the ISEA for A&A activities, system updates, and ongoing system change initiatives. The Contractor shall establish and maintain records in eMass to support system authorization.

During RMF Step 1, the Contractor shall coordinate activities with the ISSM and provide analysis to establish data types for system categorization level definitions. At Step 2, the Contractor shall develop the RMF Security Assessment Plan (SAP). At Step 3, the Contractor shall ensure the implementation of all controls, update eMASS records, and complete the documentation in preparation for RMF Step 4. At Step 4 the Contractor shall separate entry and validation duties that required for system authorization. The Contractor shall ensure that a Qualified Navy Validator conducts validation activities, coordinates efforts, and prepares system documentation for RMF Step 5. The Contractor shall provide the Cybersecurity risk assessment report. Using the assessment report provide a summary of expected Step 5 checkpoint and present results to the ISSM. During Step 5 of the RMF process, the Contractor shall compile documentation/artifacts and support collaboration meetings. During Step 6 of the RMF process, the Contractor shall update risk assessments, incorporate new capabilities into systems, and provide vulnerability assessments to maintain an authorized security posture.

Using RMF procedures, the Contractor shall generate and document automated and repeatable processes for implementation in PMW 130. The Contractor shall coordinate with PMW 130 staff to reduce the timeline to accredit system and increase the likelihood of authorization decisions at Step 5 of the RMF process.

The Contractor shall have working knowledge of the PMW 130 Configuration Management (CM), participate in the Local Change Control Board (LCCB), and follow the CM process for RMF. The Contractor shall provide input to PMW 130 Plans at the system level to meet requirements of RMF. The Contractor shall prepare IA technical baseline reports and assessments to establish consistency between systems performance and requirements.

The Contractor shall support the establishment, coordination, and accountability management of software and related DON Application and DADMS accountability database. The Contractor shall submit and maintain data in the DADMS and the DITPR-DON, which replaced the DON IT Registry. DITPR-DON is the single, authoritative source for data regarding DON IT systems.

The Contractor shall plan, conduct, and document Cross Domain Services (CDS) interactions with CDS customers from initial requirements definition, CDS selection, and CDS process documentations requirements for both Secret and Below Interoperability (SABI) and Top Secret Sensitive Compartmented Information and Below Interoperability (TSABI) processes. The Contractor shall schedule and support technical exchange meetings, support Cross Domain Technical Advisory Board (CDTAB), DSAWG and NAVINTEL IA meetings in pursuit of Cross Domain Assessment (CDA) approvals, ensure CDS customers funding and contract actions are completed, schedule CDS installations and establish go/no criteria for both CDS installations and SBSAs.

The Contractor shall provide site-specific validation and revalidation of CDS systems. The Contractor shall participate in site surveys and technical exchange meetings with Program Office, Data Owners, and Site Representatives when and where requested by the Program Office. The Contractor shall provide documentation assistance to user sites; and emulate and pretest site-specific CDS configurations and rule sets in the contractors' test laboratories. Under the auspices of each responsible Authorization Official (AO), monitor CDS installations, configurations and user training; and plan, conduct and document SBSAs. The Contractor shall plan, conduct, and document reaccreditation activities at CDS sites that require upgrades and/or annual/triennial reaccreditations.

CDRLs

- A003 RMF Step 2 Collaboration Meeting Minutes
- A004 RMF Step 5 Collaboration Meeting Minutes
- A006 RMF Step 2 Peer Review Report
- A007 RMF Step 5 Peer Review Report

4.0 CYBERSECURITY COMPLIANCE

4.1 CYBER IT AND CYBERSECURITY PERSONNEL

The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information systems. Proposed contractor Cyber IT and

cybersecurity personnel shall be appropriately qualified prior to the start of the contract performance period or before assignment to the contract during the course of the performance period.

The contractor shall identify, train, track, and report cybersecurity personnel, also known as Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel. Reporting requirements are at the task order level. Although the minimum frequency of reporting is monthly, the task order can require additional updates as requested by the Government.

The contractor employer shall ensure contracted employee receive training on new vendor, and emergent technologies for task orders on the contract. The contractor employer shall be responsible for ensuring contracted employees maintain appropriate training and certifications in accordance with DoDD 8140.01and DoD 8570.01. The contractor employer shall make certain the contracted employee maintain technical proficiency in the Navy Enterprise Network current platform – proficiency is inspect able by the Government. The contractor employer shall be responsible for required vendor training in cases where a manufacturer requires certifications. The contractor employer shall be responsible for Continuing Education Fees associated with vendor certifications.

Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form.

When a contractor requires logical access to a government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the PMW 130 Information Assurance Management (IAM) office:

1. For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil/ or http://iatraining.disa.mil/. For those contractors requiring initial training and do not have a CAC, contact the PMW 130 ACTR at phone number (858) 537-8911or e-mail questions to roc@spawar.navy.mil for additional instructions. Training is available online at https://cyber.mil.

2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the PMW 130 ACTR or from the website: https://navalforms.documentservices.dla.mil/. Route digitally signed forms to the ACTR via encrypted e-mail to roc@spawar.navy.mil.

Contractor personnel with privileged access shall be required to acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

4.2 CYBERSECURITY WORKFORCE (CSWF) REPORT

DoD 8570.01-M and DFARS PGI 239.7102-3 have promulgated that contractor personnel shall have documented current cybersecurity certification status within their contract. The Contractor shall develop,

maintain, and submit a Cybersecurity Workforce (CSWF) Report at the task order level. IAW clause DFARS 252.239-700, the Contractor shall provide a CSWF list that identifies those individuals who are IA trained and certified. Utilizing the format provided at the task order level, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. Additional reporting details and distribution instructions are at the task order level. The Contractor shall verify with the COR or other government representative the proper labor category cybersecurity designation and certification requirements.

4.2.1 Personnel Qualifications (Minimum)

Personnel assigned to or utilized by the Contractor in the performance of this contract shall, at a minimum, meet the experience, educational, or other background requirements set forth below and shall be fully capable of performing in an efficient, reliable, and professional manner. If the offeror does not identify the labor categories listed below by the same specific title, then a cross-reference list should be provided in the offeror's proposal identifying the difference.

The Government may review resumes of contractor personnel assigned to ensure that the minimum qualifications stated below are met.

If the Ordering Officer questions the qualifications or competence of any persons performing under the contract, the burden of proof to sustain that the person(s) are qualified as prescribed herein shall be upon the contractor.

The Contractor must have personnel, organization, and administrative control necessary to ensure that the services performed meet all requirements specified in delivery orders. The work history of each Contractor employee shall contain experience directly related to the tasks and functions to be assigned. The Ordering Officer reserves the right to determine if a given work history contains necessary and sufficiently detailed, related experience to reasonably ensure the ability for effective and efficient performance.

Labor Categories	**Work Location**	**Minimum Requirements**
Risk Analyst III	Contractor	8570 IAM I +NQV I (within 1 year)
Information Security Manager	Contractor	8570 IAM III equivalent
Information Security Analyst V	Contractor	8570 IAM II + NQV II or III (within 1 year)

5.0 INFORMATION TECHNOLOGY (IT) SERVICES REQUIREMENTS

5.1 INFORMATION TECHNOLOGY (IT) GENERAL REQUIREMENTS

When applicable, the contractor shall be responsible for the following:

- Confirm that no production systems are operational on any RDT&E network.
- Follow DoDI 8510.01, dated 12 Mar 2014 when deploying, integrating, and implementing IT capabilities.
- Work with government personnel to confirm compliance with all current Navy IT and cybersecurity policies, including those pertaining to DIACAP to RMF transitions.
- Follow SECNAVINST 5239.3C, dated 02 May 2016 and DoDI 8510.01, dated 28 Jul 2017 prior to integration and implementation of IT solutions or systems.
- Register contractor-owned or contractor-maintained IT systems used on contract in the DITPR-DON.

- Only perform work specified within the limitations of the contract or task order.

5.2 DON APPLICATION AND DATABASE MANAGEMENT SYSTEM (DADMS)

The Contractor shall make certain that no Functional Area Manager (FAM) disapproved applications are integrated, installed, or operational on Navy networks. The Contractor shall confirm that all databases that use database management systems (DBMS) designed, implemented, and hosted on servers and mainframes supporting Navy applications and systems be registered in DADMS and are FAM approved. Register all integrated, installed, or operational applications hosted on Navy networks in DADMS and approved by the FAM. Do not integrate, install, or operate operational systems or applications on the RDT&E network.

5.3 INFORMATION SECURITY

Pursuant to DoDM 5200.01, the Contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems used on contract. The Contractor shall disseminate unclassified DOD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the Contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

6.0 REPORTS, DATA AND DELIVERABLES

Contract Data Requirements List, DD Form 1423, shall specify reports, technical data, and computer software delivery requirements at the individual delivery/task order level.

The Contractor shall provide prototype deliverables as specified in individual task orders.

The Contractor shall protect and handle all classified deliverables in accordance with standard security practices and procedures.

The Contractor shall provide the documentation necessary to accomplish the tasks and objectives as outlined in Section 5.0. In addition, the Contractor shall deliver the following contract data requirements identified below and in Contract Exhibit A – Contract Data Requirements List.

CDRL	Name	PWS Reference
A001	Contractor's Progress, Status and Management Report (MSR)	3.0
A002	Trip/Activity Reports	12.0
A003	RMF Step 2 Collaboration Meeting Minutes	3.5
A004	RMF Step 5 Collaboration Meeting Minutes	3.5
A005	Inheritance Memorandum of Agreement (iMOA)	3.4
A006	RMF Step 2 Peer Review Report	3.5
A007	RMF Step 5 Peer Review Report	3.5
A008	System Security Plan	8.4
A009	Management Plan: Transition Plan	10.4

Material shall be prepared in accordance with DoD, DoN, or PEO formats; free of errors in content, spelling, grammar, punctuation, format, and consistency; and submitted in accordance to the schedule of the requestor.

7.0 PERFORMANCE EVALUATION

7.1 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

The QASP monitors performance and identifies the required documentation and employed resources. The QASP provides a means for evaluating whether the Contractor is meeting the performance standards and quality levels identified in the PWS. The Government will assess contract deliverables and overall Contractor performance against this plan.

8.0 SECURITY AND ACCESS

Most requirements of this PWS will be met at or below the SECRET level; however, some tasks require access to SECRET and TOP SECRET at Government and Prime Mission Product (PMP) designated Contractor facilities (an example: access to Radiant Mercury Contractor testing lab). The Contractor shall also be required to attend meetings, briefings, threat or risk and test assessments comprised of algorithms, methods and technical specifications; requirements development sessions and rapid acquisition strategies classified at the SECRET and TOP SECRET level to reach PMW 130's acquisition milestones.

In the future, approximately 2025, we anticipate the requirement to handle incidental SCI. At that time, some Contractors shall need Joint Worldwide Intelligence Communication System (JWICS) accounts.

At that point, SCI-related access will be required by contractor personnel within SCI-accredited spaces to perform the support described by this task. Additionally, Contractor personnel must have access to the CDS program SCI documentation to support this effort. It is further anticipated that the contractor will be required to meet with Government agency personnel at Government or Contractor SCI facilities to discuss CDS related security requirements and to perform system tests and evaluations. Contractor personnel must have access to the CDS installations as outlined in the travel section of this PWS.

Contractors shall hold the appropriate security clearances and accesses. Contractors must be US citizens and hold at least a TS/SI/TK/G/HCS Clearance. Security clearance requirement for personnel working on the technical tasks of this contract is TS/SI/TK/G/HCS.

Until then, at a minimum, all personnel shall possess a GENSER SECRET personal clearance and at least two personnel shall require a TOP SECRET personal clearance. In addition, the Contractor is required to access SIPRNet at Government locations (see attached DD254).

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to Commanding Officer, Attn: Foreign Travel Team, Naval Information Warfare Center Pacific, 53560 Hull Street, Building 27, 2nd Floor - Room 206, San Diego, CA 92152 for action. Submit a Request for Foreign Travel form for each traveler, in advance of the travel, to initiate the release of a clearance message at least 30 days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure. Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at Joint Knowledge Online (JKO): https://jkodirect.jten.mil/courses/atl1/, Course Number: US007, Title: Level 1 Anti-terrorism Awareness Training. If experiencing problems accessing this website contact the JKO Help Desk (24 hours a day/7 days a week, jkohelpdesk@jten.mil, 757-203-5654). Sere 100.2 Level A code of conduct training is also required prior to OCONUS travel for all personnel. Sere 100.2 Level A training can be accessed at http://jko.jfcom.mil (recommended),

https://jkodirect.jten.mil/atlas2/faces/page/login/login.seam; Recommended Course: Prefix: J3T; Course: J3TA-US1329 SERE 100.2 Level A SERE Education and Training in Support of the Code of Conduct for civilian, military, and contractors. Personnel utilizing this site must have a CAC. A Sere 100.2 Level A training disk is available at the PMW 130 Point Loma Office or Old Town Campus Office. Specialized training for specific locations, such as SOUTHCOM human rights, or U.S. forces Korea entry training might also be required. PMW 130 security personnel will inform you if there are additional training requirements.

Finally, European Command (EUCOM) has mandated that all personnel going on official travel to the EUCOM Area of Responsibility (AOR) must now register with the Smart Traveler Enrollment Program (STEP). When you sign up, you will automatically receive the most current information the State Department compiles about your destination country. You will also receive updates, including Travel Warnings and Travel Alerts. Sign up is one-time only, after you have established your STEP account, you can easily add official or personal travel to anywhere in the world, not just EUCOM. http://travel.state.gov/content/passports/en/go/step.html.

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems used on contract. The Contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

8.1 OPERATIONS SECURITY

OPSEC is a five-step analytical process (identify critical information, analyze the threat, analyze vulnerabilities, assess risk, and develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce, or process Critical Information or Critical Program Information, and therefore all personnel must practice OPSEC. All work is to be performed in accordance with DoD and OPSEC requirements and in accordance with the OPSEC attachment to the DD254.

8.1.1 IT Position Categories

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. As defined in DoD 5200.2-R, SECNAVINST 5510.30 and SECNAV M-5510.30, three basic DoN IT levels/Position categories exist:

- IT-I (Privileged access)
- IT-II (Limited Privileged, sensitive information)
- IT-III (Non-Privileged, no sensitive information)

Note: The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (as used in DoD 5200.2-R, Appendix 10).

Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The Contractor PM shall assist the Government Project

Manager or COR in determining the appropriate IT Position Category assignment for all contractor personnel. All required Single-Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), and National Agency Check (NAC) adjudication are required, pursuant to DoDI 8500.01 and SECNAVINST 5510.30. SPAWAR/NIWC Atlantic/NIWC Pacific Security Office, processed by the OPM, and adjudicated by DOD CAF submits requests for investigation of contractor personnel for fitness determinations or IT eligibility without classified access. IT Position Categories are determined based on the following criteria:

8.1.1.1 IT-I Level (Privileged)

Positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudication of Single Scope Background Investigation (SSBI) or SSBI-PR. The SSBI or SSBI-PR is updated a minimum of every 5 years. Assignment to designated IT-I positions requires U.S. citizenship unless a waiver request is approved by CNO.

8.1.1.2 IT-II Level (Limited Privileged)

Positions in which the incumbent is responsible for the-direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the IT-II Position level to insure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudication of a Position of Trust National Agency Check with Law and Credit (PT/NACLC). CNO approves waivers for assignment to designated IT-II positions that require U.S. citizenship, if needed.

8.1.1.3 IT-III Level (Non-privileged)

All other positions involved in computer activities. Incumbent in this position has non-privileged access to one or more DoD information systems/applications or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudication of a Position of Trust National Agency Check with Written Inquiries (PT/NACI).

Note: A minimum of five Certification and Accreditation (C&A) Engineers formally designated as Radiant Mercury Trusted Agents (TA) by the Defense Intelligence Agency and NAVINTEL IA are required for this effort.

8.2 DOD INFORMATION ASSURANCE AWARENESS TRAINING

The Contractor shall complete DoD IA Awareness training annually. NAVWAR has elected to use the Cyber Awareness Challenge training to meet the requirement identified in DoD Directive 8570.01, which is accessible through the Total Workforce Management System (TWMS). The policy applies to all Team NAVWAR computer and network users located at NAVWAR Headquarters, affiliated PEOs, and Business Units to include all civilians, military, and Industry Partners. This policy may also apply to the tenant Command personnel, by agreement. The Contractor shall provide a signed certificate for the annual IA Awareness training upon request. TWMS is located at https://twms.nmci.navy.mil.

8.3 INFORMATION ASSURANCE AND PERSONNEL SECURITY REQUIREMENTS FOR ACCESSING NAVY ENTERPRISE RESOURCE PLANNING (ERP) MANAGEMENT SYSTEM

Contractor personnel assigned to perform work under this contract may require access to Navy Enterprise Resource Planning System. Prior to accessing NERP System, Contractor personnel shall contact the applicable NMCI Assistant Customer Technical Representative (ACTR) and obtain an NMCI account. ACTRs can be found on the NMCI Homeport website at: https://nmcicustomerreporting/CTR_Lookup/index.asp. Once an NMCI account has been established, the Contractor shall submit a request for Navy ERP access and the role required via the Contracting Officer's Representative (COR) to the Competency Role Mapping Point of Contact (POC). The COR will validate the need for access, make certain all prerequisites are completed and with the assistance of the Role Mapping POC, identify the Computer Based Training requirements needed to perform the role assigned. Items to complete prior to requesting a role for Navy ERP include: Systems Authorization Access Request, DD Form 2875, Dated Oct 2007, Annual IA training certificate, and favorably adjudicated Trustworthiness Investigation commensurate with the appropriate IT Category (requires the SF85P).

For this procedure, reference to the COR shall mean the Procuring Contracting Officer for contracts that do not have a designated COR. For directions on completing the SF85P, the Contractor is instructed to consult with their company's Security Manager. In order to maintain access to required systems, the Contractor shall certify completion of annual IA training, monitor expiration of requisite background investigations and initiate re-investigations.

8.4 SYSTEM SECURITY PLAN AND ASSOCIATED PLANS OF ACTION

8.4.1 Protecting Controlled Unclassified Information

Upon request, the Contractor shall provide the Government a system security plan (or extract thereof) and any associated plans of action developed to satisfy the adequate security requirements of DFARS 252.204-7012. The plan must be in accordance with NIST Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" that was in effect at the time the solicitation is issued or as authorized by the Contracting Officer. The plan will describe the Contractor's unclassified information system(s) and network(s) where Covered Defense Information (CDI) associated with the execution and performance of this contract is processed, stored, or transmits System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System. (CDRL A003)

8.4.2 Access to System Security Plan(s)

Upon request, the Contractor shall provide the Government with access to the system security plan(s) (or extracts thereof) and any associated plans of action for each of the Contractor's tier one level subcontractor(s), vendor(s), and supplier(s), and the subcontractor's tier one level subcontractor(s), vendor(s), and supplier(s), who process, store, or transmit CDI associated with the execution and performance of this contract, System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System.

8.5 COMMON ACCESS CARDS (CACS)

The Government will provide CACs for the performance of this task order. The Contractor PM/FSO is responsible for notifying the COR and the Trusted Agent (TA) when an employee who has been issued a CAC leaves the Company or transfers to another Program/Project. In the case of an employee who no longer works for the company, the company shall collect the CAC and turn it over to the TA within two

working days of the employee's departure. In the case of an employee still retained by the company transferring to another Program/Project with-in NAVWAR, the company shall notify the COR and the TA within two working days so the TA can transfer the TA responsibilities to the new TA vice revoking and issuing a new CAC.

8.6 CONTRACTOR PICTURE BADGE

A contractor picture badge may be issued to contractor personnel by NAVWARSYSCOM upon receipt of a valid visit request from the Contractor and a picture badge request from the COR. A list of personnel requiring picture badges must be provided to the COR to verify that the contract or delivery/task order authorizes performance at NAVWARSYSCOM prior to completion of the picture badge request.

The Contractor assumes full responsibility for the proper use of the identification badge and is responsible for the return of the badge upon termination of personnel or expiration or completion of the contract.

At the completion of the contract, the contractor shall forward to NAVWARSYSCOM a list of all unreturned badges with a written explanation of any missing badges.

9.0 GOVERNMENT FURNISHED PROPERTY

GFP is not anticipated.

10.0 TASK ORDER MANAGEMENT AND ADMINISTRATION

10.1 WIDE AREA WORK FLOW (WAWF) INVOICING REQUIREMENTS

The Contractor shall notify the COR via e-mail when the Contractor submits invoices to WAWF. The Contractor shall also provide a soft copy of the invoice and supporting documentation as requested by the COR in order to validate the invoiced amount against the services provided during the billing cycle and completing the Invoice Review Form provided.

10.2 CONTRACTOR EMPLOYEE IDENTIFICATION

Contractor employees must be clearly identifiable while on Government property by wearing appropriate badges. Contractor personnel and their subcontractors must identify themselves as contractors or subcontractors during meetings, telephone conversations, in electronic messages, or correspondence related to this contract.

Contractor-occupied facilities (on Department of the Navy or other Government installations) such as offices, separate rooms, or cubicles must be clearly identified with Contractor supplied signs, name plates or other identification, showing that these are work areas for Contractor or subcontractor personnel.

10.3 MANDATORY TRAINING

Contractor personnel shall complete all mandatory training requirements per the NAVWAR Code 80330 Mandatory Training Wiki:
https://wiki.spawar.navy.mil/confluence/display/HQ/Employee+Mandatory+Training

The Contractor is responsible for collecting and reporting the training status of all personnel, including subcontractor personnel. The Contractor shall report individual contractor personnel training status by updating Contractor's Progress, Status, and Management Reports CDRL (A001), Staffing Plan

attachment.

10.4 POST AWARD CONFERENCE

The Contractor shall participate in a Post Award Conference (PAC) within ten working days after task order award to establish points of contact, discuss terms and conditions of the task order, and to provide the Government with their detailed transition plan. (CDRL A009) The transition plan shall include a list of personnel ready to start performing with the performance start date, introduction of the Prime and Subcontractor team, the staffing plan and timeline, and steps the company will take to ensure a smooth transition. A Staffing Requirements Priority List (SRPL) will be provided to the Contractor at the PAC.

Initial performance shall start no later than five business days after task order award. All Priority One personnel identified on the updated SRPL shall start performance no later than 10 business days after receipt of the SRPL. All remaining personnel required on the updated SRPL shall start performance no later than 30 days after receipt of the SRPL.

10.5 WORKWEEK

The normal workweek for Government employees at NAVWARSYSCOM is Monday through Friday 0700-1630 with core hours of Monday through Friday 0900-1500.

Unless otherwise specified, the Contractor's work shall be performed within the normal workweek. Pursuant to Federal law (5 U.S.C. 6103) the following public holidays are observed by the Government:

Name of Holiday	**Time of Observance**
New Year's Day	1 January
Martin Luther King Jr. Day	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

If any of the above public holidays fall on a non-workday – Saturday or Sunday – the holiday usually is observed on Monday (if the holiday falls on Sunday) or Friday (if the holiday falls on Saturday).

NOTICE: Contractor employees who make repeated deliveries to military installations shall obtain the required access card via the Defense Biometric Identification System (DBIDS) system. Information about DBIDS can be found at https://dbids-global.dmdc.mil/enroll#!/

10.6 LIABILITY INSURANCE—FIXED PRICE CONTRACTS OR COST REIMBURSEMENT (See FAR Provision 28.307-2)

The following types of insurance are required in accordance with the FAR 52.228-5 "Insurance—Work on a Government Installation" clause and shall be maintained in the minimum amounts shown:

(1) Workers' compensation and employers' liability: minimum of $100,000

(2) Comprehensive general liability: $500,000 per occurrence
(3) Automobile liability: $200,000 per person
$500,000 per occurrence
$20,000 per occurrence for property damage

Upon notification of contract award, the Contractor shall furnish to the Contracting Officer, as defined by paragraph (b) of the FAR 52.228-5 "Insurance—Work on a Government Installation" clause, a certificate or written statement of insurance prior to commencement of work under this contract. The written statement of insurance must contain the following information: policy number, policyholder, carrier, amount of coverage, dates of effectiveness (i.e., performance period), and contract number. The contract number shall be cited on the certificate of insurance.

10.7 REQUIRED INFORMATION ASSURANCE AND PERSONNEL SECURITY REQUIREMENTS FOR ACCESSING GOVERNMENT INFORMATION SYSTEMS AND NONPUBLIC INFORMATION

(a) Definition. As used in this clause, "sensitive information" includes:
(i) All types and forms of confidential business information, including financial information relating to a contractor's pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;
(ii) Source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 423);
(iii) Information properly marked as "business confidential," "proprietary," "procurement sensitive," "source selection sensitive," or other similar markings;
(iv) Other information designated as sensitive by the NAVWARSYSCOM.

(b) In the performance of the contract, the Contractor may receive or have access to information, including information in Government Information Systems and secure websites. Accessed information may include "sensitive information" or other information not previously made available to the public that would be competitively useful on current or future related procurements.
(c) Contractors are obligated to protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the contract, whether the information comes from the Government or from third parties. The Contractor shall—
(i) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the contract, and not for any other purpose unless authorized;
(ii) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract or as authorized by Federal statute, law, or regulation;
(iii) Inform authorized users requiring access in the performance of the contract regarding their obligation to utilize information only for the purposes specified in the contact and to safeguard information from unauthorized use and disclosure.
(iv) Execute a "Contractor Access to Information Non-Disclosure Agreement," and obtain and submit to the Contracting Officer a signed "Contractor Employee Access to Information Non-Disclosure Agreement" for each employee prior to assignment;
(v) Notify the Contracting Officer in writing of any violation of the requirements in (i) through (iv) above as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

(d) In the event that the Contractor inadvertently accesses or receives any information marked as "proprietary," "procurement sensitive," or "source selection sensitive," or that, even if not properly marked otherwise indicates the Contractor may not be authorized to access such information, the Contractor shall (i) Notify the Contracting Officer; and (ii) Refrain from any further access until authorized in writing by the Contracting Officer.

(e) The requirements of this clause are in addition to any existing or subsequent Organizational Conflicts of Interest (OCI) requirements which may also be included in the contract, and are in addition to any personnel security or Information Assurance requirements, including Systems Authorization Access Request (SAAR-N), DD Form 2875, Annual Information Assurance (IA) training certificate, SF85P, or other forms that may be required for access to Government Information Systems.

(f) Subcontracts. The Contractor shall insert paragraphs (a) through (f) of this clause in all subcontracts that may require access to sensitive information in the performance of the contract.

(g) Mitigation Plan. If requested by the Contracting Officer, the Contractor shall submit, within 45 calendar days following execution of the "Contractor Non-Disclosure Agreement," a mitigation plan for Government approval, which shall be incorporated into the contract. At a minimum, the mitigation plan shall identify the Contractor's plan to implement the requirements of paragraph (c) above and shall include the use of a firewall to separate Contractor personnel requiring access to information in the performance of the contract from other Contractor personnel to ensure that the Contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A "firewall" may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The Contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

11.0 CONTRACTING OFFICER'S REPRESENTATIVE

Refer to contract.

12.0 TRAVEL

The Contractor shall use the electronic Travel Request form (provided separately) for all required travel in this task order. The request for all routine travel shall be made via email to the COR no later than five working days in advance of travel date for final approval. For emergent travel, requests shall be made within three days of the actual travel date and will be approved by the COR verbally. The Contractor shall follow-up with the electronic travel request within five working days of the original request. Trip and Activity Reports shall be completed and submitted to the COR 10 days after completion of trip per the CDRL.

Due to the nature of this effort, the contractor may be required to travel extensively. The contractor shall travel to support various installations, to include operational locations, both within CONUS and OCONUS. Reimbursement will be in accordance with the Joint Travel Regulations (JTR). The following table is an estimate of travel requirements for a one-year period; however, this will vary depending on the dynamic requirements of the program office.

From	To	Number of Trips	Number of People	Number of Days
TBD	Aberdeen PG, MD	4	1	5
TBD	Bahrain	2	1	7
TBD	Bath, MD	1	1	5
TBD	Boulder, CO	2	1	5
TBD	China Lake, CA	4	1	5
TBD	Colorado Springs, CO	4	1	5
TBD	Denver, CO	6	1	5
TBD	Eglin AFB, FL	2	1	5
TBD	Fort Bliss, TX	2	1	5
TBD	Fort Buckner, Japan	1	1	7
TBD	Fort Detrick, MD	1	1	5
TBD	Fort Hood, TX	2	1	5
TBD	Fort Irwin, CA	2	1	5
TBD	Fort Meade, MD	5	1	5
TBD	Fort Polk, LA	1	1	5
TBD	Grafenwoeher, GE	4	1	7
TBD	Hill AFB, UT	1	1	5
TBD	Hohenfels, GE	1	1	5
TBD	Holloman AFB, NM	1	1	5
TBD	Honolulu, HI	4	1	5
TBD	Hunt Valley, MD	1	1	5
TBD	Kirtland AFB, NM	1	1	5
TBD	Lackland AFB, TX	1	1	5
TBD	Miami, FL	2	1	5
TBD	Mayport, FL	3	1	5
TBD	Naples, Italy	3	1	7
TBD	Nellis AFB, NM	1	1	5
TBD	Nashua, NH	1	1	5
TBD	Norfolk, VA	8	1	5
TBD	Orlando, FL	2	1	5
TBD	Phoenix, AZ	2	1	5
TBD	Point Mugu, CA	2	1	5
TBD	Portsmouth, RI	1	1	5
TBD	Molesworth, England	2	1	7
TBD	Qatar	1	1	7
TBD	San Diego, CA	8	1	5
TBD	Sasebo, JP	2	1	7
TBD	Seoul, South Korea	3	1	7
TBD	Taunton, MA	2	1	5
TBD	Tucson, AZ	2	1	5

TBD	UAE	1	1	7
TBD	Virginia Beach, VA	2	1	5
TBD	Waco, TX	2	1	5
TBD	Wiesbaden, GE	2	1	5
TBD	Yokosuka, Japan	4	1	5

CDRLs

- A002 Trip/Activity Reports

The travel request shall include the following:

- Traveler's Name
- Name of specific Government Technical POC requesting the travel
- Program and project name travel is required for
- Applicable PWS Paragraph number
- Reason for travel
- Duration of travel
- Dates of travel
- Travel cost estimate
- Total travel funds expended to date
- Balance of authorized travel funding

The Government authorizes travel outside the regularly scheduled workday as a work activity for the contract as defined in contract clause H-6 Reimbursement of Travel Costs (e.g. weekend and evening travel).

13.0 PLACE AND PERIOD OF PERFORMANCE

13.1 PLACE OF PERFORMANCE

The place of performance for efforts under this performance work statement shall be at the Contractor's facilities and at Government facilities as designated by PMW 130 Program Office in the San Diego, CA area.

13.2 PERIOD OF PERFORMANCE

The period of performance for this Task Order is five years (one base year and four one-year options).

14.0 ENTERPRISE CONTACTOR MANPOWER REPORTING APPLICATION (ECMRA)

The Contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for PMW 130 via a secure data collection site. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

(1) W, Lease/Rental of Equipment;
(2) X, Lease/Rental of Facilities;
(3) Y, Construction of Structures and Facilities;

(4) D, Automatic Data Processing and Telecommunications, IT and Telecom-Telecommunications Transmission (D304) and Internet (D322) ONLY;
(5) S, Utilities ONLY;
(6) V, Freight and Shipping ONLY.

The contractor is required to completely fill in all required data fields using the following web address: www.ecmra.mil.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. Report inputs any time during the FY, however, report all data no later than October 31 of each calendar year. Contractors may direct questions to the help desk at www.ecmra.mil.

For the purposes of CMRA reporting, the Federal Supply Code/Product Service Code applicable to the contract is D310 at the Task Order Level.

15.0 PERFORMANCE MATRIX

Objective	PWS Paragraph	Acceptable Quality Level
Trip/Activity Reports: The Contractor shall provide a trip/activity report to the COR via email no later than 10 days after a trip is complete.	12	Delivery in the allotted time period meets a "Satisfactory" level of quality.
RMF Step 2 Collaboration Meeting Minutes delivery: The Contractor shall deliver comprehensive meeting minutes no later than 2 days after scheduled RMF Step 2 Collaboration Meeting.	3.5	Minutes are delivered to the Government and attached to the eMASS instance as an artifact no later than 2 days after the scheduled RMF Step 2 Collaboration Meeting and require no more than one adjustment request before concurrence is received by the Government.
RMF Step 5 Collaboration Meeting Minutes delivery: The Contractor shall deliver comprehensive meeting minute no later than 2 days after scheduled RMF Step 5 Collaboration Meeting.	3.5	Minutes are delivered to the Government and attached to the eMASS instance as an artifact no later than 2 days after the scheduled RMF Step 5 Collaboration Meeting and require no more than one adjustment request before concurrence is received by the Government.
Inheritance Memorandum of Agreement (iMOA) delivery: The Contractor shall complete the iMOA for the given system and deliver via email to the ISSM and the SCA Liaison.	3.4	Delivery of the completed iMOA to the ISSM and the SCA Liaison via email and attachment to eMass as an artifact no less than 10 days prior to the scheduled collaboration meeting of Checkpoint 5.
RMF Step 2 Peer Review Report delivery: The Contractor shall complete the RMF Step 2 Peer Review Checklist no less than 2 days after the RMF Step 2 Peer Review.	3.5	Delivery of the RMF Step 2 Peer Review Checklist to the ISSM and attachment to the eMass package as an artifact no less than 2 days after the RMF Step 2 Peer Review.
RMF Step 5 Peer Review Report Delivery: The Contractor shall complete the RMF Step 5 Peer Review Report no	3.5	Delivery of the RMF Step 5 Peer Review Checklist to the ISSM and attachment to the eMass package as an artifact no later than 2 days after the RMF Step 5 Peer Review.

Objective	PWS Paragraph	Acceptable Quality Level
less than 2 days after the RMF Step 5 Peer Review.		
System Security Plan Delivery: The SAP must be complete and ready for review no less than 5 days prior to the RMF Step 2 Scheduled Collaboration.	8.4	Delivery of the SAP to the eMASS instance of the given system no later than 5 days prior to the RMF Step 2 Scheduled Collaboration.
DITPR DON Annual Inspection Reviews: Annual DITPR DON/DADMS inspections requirements must be completed on time.	3.5	Completion of the DITPR DON/DADMS annually inspection requirement by the deadline date represents a "Satisfactory" level of quality.
Generation of Authorization Stipulation POAM and management through the stipulation timeline: The Contractor shall generate a POAM of Authorization stipulations and manage the POAM to completion.	3.5	Management of the completion of system Authorization POAM within the stipulated time period demonstrates a "Satisfactory" level of quality
Provide updates to baselined IMS schedules: The Contractor shall develop system activities and establish RMF authorization schedules to ensure accuracy of the IMS and address RMF schedule changes.	3.2	Management of changes to IMS baseline schedules to ensure accuracy within 30 days of established RMF Step 5 completion date.

1
2

1 **GLOSSARY**
2

A&A	Assessment and Authorization
ACAT	Acquisition Category
ACTR	Assistant Contract Technical Representative
AO	Authorization Official
AOR	Area of Responsibility
AT/FP	Anti-Terrorism/Force Protection
C4I	Command, Control, Communications, and Intelligence
CAC	Common Access Cards
CARD	Cost Analysis Requirements Description
CAP	Contractor Acquired Property
CDA	Cross Domain Assessment
CDI	Covered Defense Information
CDRL	Contract Data Requirements List
CDS	Cross Domain Services
CDSO	Cross Domain Service Office
CDTAB	Cross Domain Technical Advisory Board
CM	Configuration Management
CMPro	Configuration Management Professional
CND	Computer Network Defense
COCOM	Combatant Command
COR	Contracting Officer's Representative
COTS	Commercial Off-The-Shelf
CS	Cybersecurity
CSWF	Cybersecurity Workforce
CUI	Controlled Unclassified Information
DADMS	DON Application and Database management System
DBIDS	Defense Biometric Identification System
DBMS	Database management Systems
DGSIT	Deploying Group System Integration Testing
DIA	Defense Intelligence Agency
DIACAP	Defense Information Assurance and Accreditation Process
DISA	Defense Information Systems Agency
DITPR-DON	Department of Defense IT Portfolio Registry – Department of the Navy
DODIN	Department of Defense Information Network
DSAWG	Defense Security/Cybersecurity Authorization Working Group
ECMRA	Enterprise Contractor Manpower Reporting Application

eMASS	Enterprise Mission Assurance Support Service
EUCOM	European Command
FAM	Functional Area Manager
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GENSER	General Services
GFP	Government Furnished Property
GOTS	Government Off-The-Shelf
IA	Information Assurance
IAM	Information Assurance Management
IAW	in accordance with
IDEA	Information Dominance Enterprise Architecture
IMS	Integrated Master Schedule
IPS	Intrusion Prevention Systems
IPT	Integrated Product Team
IRRs	Installation Readiness Reviews
ISEA	In-Service Engineering Agent
ISSM	Information Systems Security Manager
IT	Information Technology
IV&V	Independent Validation and Verification
JIE	Joint Information Environment
JKO	Joint Knowledge Online
JWICS	Joint Worldwide Intelligence Communication System
KM	Key Management
LCCB	Local Change Control Board
MOA	Memoranda of Agreement
MOE	Measures of Effectiveness
MOU	Memoranda of Understanding
NAVIFOR	Naval Information Forces
NAVINTEL	Naval Intelligence
NAVWAR	Naval Information Warfare
NAVWARSYSCOM	Naval Information Warfare Systems Command
NERP	Navy Enterprise Resource Planning
NGEN	Next Generation Enterprise Network
NIA	NAVINTEL Information Assurance
NISPOM	National Industrial Security Program Operating Manual
NMCI	Navy-Marine Corps Intranet
NSA	National Security Agency

NTD	Navy Telecommunications Directive
OCI	Organizational Conflicts of Interest
OCONUS	Outside the Continental United States
OM&S	Operating Materials and Supplies
ONE-NET	OCONUS Naval Enterprise Network
OPSEC	Operations Security
PAA	Privileged Access Agreement
PEO	Program Executive Office
PKI	Public Key Infrastructure
PLCCE	Program Life-Cycle Cost Estimate
PMP	Prime Mission Product
PMRs	Program Management Reviews
PMW	Program Manager, Warfare
POC	Point of Contact
PP&E	Property, Plant and Equipment
PSC	Product Service Code
PSP	Personnel Security Program
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
RMF	Risk Management Framework
SAAR	System Authorization Access Request
SAAR-N	System Authorization Access Request Navy
SABI	Secret and Below Interoperability
SAP	Security Assessment Plan
SBSA	Site-Based Security Assessment
SCI	Secure Compartmented Information
SES	Senior Executive Service
SPIDER	SPAWAR PEO Integrated Data Environment and Repository
SOW	Statement of Work
SRPL	Staffing Requirements Priority List
STEP	Smart Traveler Enrollment Program
STIG	Security Technical Implementation Guide
T&E	Test and Evaluation
TA	Trusted Agent
TEMP	Test and Evaluation Master Plan
TIMs	Technical Interchange Meetings
TRRs	Test Readiness Reviews
TS	Top Secret

TSABI	Top Secret and Below Interoperability
TYCOM	Type Commander
VPN	Virtual Private Networks
WAWF	Wide Area Work Flow

1